Strelkov Stanislav Sergeevich
Student
Ural Federal University
Russia, Ekaterinburg
Academic supervisor: Zarifullina Darya Pavlovna

CLOUD STORAGE

Abstract. *Despite the many benefits of cloud storage, data protection is still a vulnerability. In this article, several ways of protection personal data on a cloud server are conceded. Data can be protected from alteration by unauthorized people using a cloud storage system, where data is encrypted and searched for using a keyword. In this article, a reliable and secure cloud storage schema using multiple service providers is examined and the system architecture of an attribute-based cloud storage system with secure provenance is described. .*

Keywords: *cloud storage, security, data, cloud server, cloud service provider, erasure code.*

Стрелков Станислав Сергеевич
Студент
Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Зарифуллина Дарья Павловна

ОБЛАЧНОЕ ХРАНИЛИЩЕ

Аннотация. *Несмотря на многочисленные преимущества облачного хранилища, защита данных по-прежнему является уязвимостью. В этой статье рассматриваются несколько способов защиты личных данных на*

облачном сервере. Данные могут быть защищены от изменений, посторонними лицами с помощью облачной системы хранения, где данные шифруются и поиск осуществляется по ключевому слову. В статье исследуется надежная и безопасная схема облачного хранилища с использованием нескольких обслуживающих компаний, и описывается архитектура облачной системы хранения на основе атрибутов с безопасным происхождением.

Ключевые слова: *облачное хранилище, безопасность, данные, облачный сервер, поставщик службы облачных вычислений, помехоустойчивый код.*

Today, cloud service technologies have gained immense popularity. Cloud storage is attracting more and more users because it performs several important functions: storage of large amounts of data, security of storage and use of data, the ability to use this data anytime and anywhere.

Both individuals and businesses use cloud storage, they store a lot of important information there, including personal data. Therefore, keeping your data safe is an important part of cloud storage. The relevance of data protection lies in a huge amount of information that should not get to attackers. New ways of protecting data appear every day, but at the same time, methods of hacking cloud storage are also improving.

The purpose of this research is to explore new ways of protecting data on a cloud server and to learn their modes of action and effectiveness.

There are several tasks to accomplish to secure your personal data in the cloud:

- to explore ways to protect information when uploading data to the server;
- to analyze data protection on the cloud storage itself;
- to consider other ways to protect user data.

First of all, in order to protect yourself from the loss of personal data from the cloud storage, you need to take care of reliable data protection when uploading to the server. It is also worth reducing the modification chance, this is necessary if someone outsiders log into the data owner's account.

To address these issues, consider a new construction of the cloud storage. In this architecture there are mainly 3 modules:

- clients;
- third party auditor;
- cloud service provider.

Clients: the data owner, which uses the cloud storage servers to store their data and depends on the cloud to manage their data files.

Third party auditor: third-party auditor is also called as cloud audit server. And this TPA is used for generating the tags before storing into the cloud service provider.

Cloud service provider: cloud service provider manages all the cloud storage servers and this CSP has efficient storage [2].

If the login credentials of the owner are hacked by the hackers and if they modify any data of the owner this modified data can be identified by the TPA when the data owner puts the request to the TPA for verifying the data. If data is not modified, then TPA generates the report. But if the data is modified then TPAR generates the report on the modified data and this report is sent to the data owner. This generated report consists of results about either owner changed the data or the cloud server changed the data. Then the owner will check the verification status of the verification request file.

So, to overcome to reduce the possibility for the uploaded data uses an approach when the owner's uploaded files can be visible to him only after searching with a keyword. If the searched word is available in the uploaded file, then it will show the particular file. Here the binary search algorithm for searching the keyword in the file and order preserving encryption (OPE) is used for encryption of the uploaded file. Order-preserving encryption (OPE) is a symmetric encryption scheme whose encryption function preserves the numerical ordering of the plaintexts.

Today, almost all the cloud service providers (CSP) have implemented fault-tolerant mechanisms at their server sides to recover original data from service failure. However, such mechanisms are of no use for users to ensure the reliability and security of their cloud data when major cloud services fail. To achieve high reliability and

security of critical data, users should not depend upon a single cloud service provider. The authors of the article «A Reliable and Secure Cloud Storage Schema Using Multiple Service Providers» propose an approach that can provide security and fault tolerance to the user's data from the client-side [1].

They propose a reliable and secure cloud storage schema using multiple CSPs. The major component of this system is the cloud storage application that uses erasure codes to encode and decode file pieces at the client-side, and upload and download encoded file pieces concurrently at multiple cloud services. When a user wants to upload a file into the cloud, the application first splits the file into multiple data pieces, and then encode them into an optimal number of checksum pieces using the erasure coding technique.

On the other hand, when a user wants to download a stored file, the application will first try to download the data pieces from the multiple cloud storage concurrently. If all data pieces are available, they can be efficiently combined into the original file without any additional decoding process. However, in the case when one or more service provider fails, the application must automatically download all available data pieces and available checksum pieces. Note that the checksum pieces serve as the redundancy of the original file, which makes our approach reliable and fault tolerant.

Fault tolerance of cloud data is commonly achieved through simple data replication. Multiple copies of original data have to be maintained on different cloud servers in order to make data more reliable. However, data replication now becomes highly unfeasible due to its low space efficiency and the ever-increasing amount of cloud data. Erasure codes, also known as forwarding error correction codes, manage to overcome the disadvantages of the data replication approach and can achieve a high degree of fault tolerance with a much lower cost of physical storage. They can be very efficient in providing fault tolerance for large quantities of data, hence they are quite suitable for large-scale cloud storage systems.

Data redundancy through parity codes represents the simplest form of erasure codes, which overcomes the drawback of data replication. RAID-5 is the most used

technique that uses parity codes. It calculates parities from the original data to achieve fault tolerance.

The architecture of the attribute-based cloud storage system with secure provenance involves four types of entities: data providers, system administrator, cloud and data users. The system administrator, who generates a master private key and publishes the corresponding public parameter, issues every data provider/user a private attribute key that is associated with his attributes and identification information. A data provider/user may be authorized to read, write to or modify the data. When sending a storage request, a data provider/user encrypts the document under an access policy over a set of attributes and subtly signs the encrypted document using his private attribute key without leaking his identity information. To read the encrypted data, a data provider/user decrypts the ciphertext using his private attribute key if his attributes satisfy the access policy associated with the ciphertext. If the data provider/user intends to write to or modify the data, after processing the data, he creates a ciphertext and attaches a signature to the ciphertext. The cloud checks the validity of the signature without learning the signer's identity and accepts the storage request if the signature is a valid one [3].

To sum up, the research results show new ways of data protection in cloud storage. Data protection while uploading to the server is achieved by using order-preserving encryption. Attribute-based cloud storage protects data on the server and addresses some of the issues on existing servers such as excessive performance overhead and lack of support for dynamic user management and lack the expressiveness in access control. Achieving fault tolerance of user data on the client side is implemented by splitting data between several cloud servers.

REFERENCES

1. Haiping Xu, Deepti Bhalerao. A Reliable and Secure Cloud Storage Schema Using Multiple Service Providers // Knowledge Systems Institute Graduate School –

2018. – Text: electronic. – URL: https://www.researchgate.net/publication/300540521_A_Reliable_and_Secure_Cloud_Storage_Schema_Using_Multiple_Service_Providers (Reference date 25.10.2020).

2. Shankar, Syed Inthiyaz, Syed Shameem. Cloud data Search and verification using Order Preserving Encryption // World Academy of Research in Science and Engineering – 2020. – Text: electronic. – URL: http://www.warse.org/IJSAIT/ (Reference date 15.12.2020).

3. Robert H. Deng, Yingjiu Li, Hui Cui Attribute-based cloud storage with secure provenance over encrypted data // Elsevier B.V – 2018. – Text: electronic. – URL: https://ink.library.smu.edu.sg/sis_research/3899/ (Reference date 18.11.2020).